日本の経済安全保障の推進に関する
BSA｜ザ・ソフトウェア・アライアンスからの提言

2022年4月26日

総論

BSA | The Software Alliance （BSA |ザ・ソフトウェア・アライアンス[1]、以下、「BSA」）は、特定社会基盤役務の安定性を強化し、関連するセキュリティ・リスクを管理することで、特定社会基盤役務を危険にさらす妨害行為や、その他の侵略的行為に対する日本の脆弱性を低減することを目指す日本政府の取り組みを支持します。

日本政府が「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」の制定に向けて審議を進め、新たな事前審査制度を実施する上での基本方針の策定、また、審査対象となる特定の役務、事業者、重要設備、重要設備の維持管理の委託を指定するにあたり重要となるのは、この新たな制度が保護しようとする技術や経済活動が阻害されるような意図せぬ結果を最小限に抑えることであり、また、これらの政策がイノベーションや世界的に利用可能な最高水準の技術へのアクセスを妨げないように保証することです。

BSA は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSA の会員は世界で最もイノベーティブな企業で構成されており、クラウドコンピューティング、データアナリティクス、人工知能（AI）など、政府や企業を強化する最先端のテクノロジーと役務を提供しています。BSA の会員は、セキュリティ分野のリーダーでもあり、今日、業界全体で使用されているソフトウェアセキュリティのベストプラクティスの多くを開拓してきました。[2]

BSA は、サイバーセキュリティ政策の策定において世界中の政府と緊密に連携しています。これらの経験に基づき、日本政府の取り組みを支援するために、以下の見解と提言を述べさせて頂きます。まず、我々は、日本政府がリスク管理への効果的なアプローチを採用することを

---

[1]BSAの活動には、 Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] *Strengthening Trust, Safeguarding Digital Transformation: BSA’s Cybersecurity Agenda* （https://www.bsa.org/files/policy-filings/10132021bsacybersecurityagenda.pdf）また、 *The BSA Framework for Secure Software: A New Approach to Security the Software Lifecycle – Version 1.1 (September 2020)* （https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf）をご覧ください。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

推奨します。そのためには、今日のテクノロジーがグローバルで相互接続された性質を持つことや、それらに対する脅威を認識すること、また、悪意ある行為を効果的に特定し遮断するために、持続可能で透明性がある政策対応の設計が必要となってきます。我々は、日本のデジタル経済の安全性、完全性、そして、活力を強化するために、日本政府に協力していけることを期待しています。

活発な意見聴取や頻繁な見直しを含む、透明性のあるプロセスを確保すること

軽減しようとする脅威に対し、どのような政策が有効であるかを理解するには、産業界を含む、影響を受ける利害関係者とのオープンで率直な対話が必要となってきます。日本政府が政策の策定と実施において、そのプロセスを透明化し、意見交換や意見募集を通して民間分野を関与させることを強く推奨します。セキュリティに関する懸念に対応する上で、産業界が以前にも増してリーダーシップを発揮する中、日本政府が、政策実施後の定期的な見直しによって、経済安全保障の確保とリスク管理のためのベストプラクティス開発を目的とした、官民連携の創造的な機会を取り入れることを奨めます。

政策の対象範囲を狭め、限定的とすること

政策がその目標を効果的に達成するためには、日本国の利益への阻害を最小限に抑え、特定の目標に対処するよう的を絞るべきであります。そのためには、政策の実施が非現実的かつ非効果的となるような、過度に広い範囲を対象とすることを避けなくてはなりません。主務省庁が特定の社会基盤役務、事業者、設備、設備の維持管理の委託の指定を検討する際、事業者が製品や役務の導入の遅れを最小限にとどめられるよう、また、イノベーションを損なわないよう、対象事業者、設備、役務等の範囲を最も必要なものに限定することを強く奨めます。

政策の一貫性と全体性を確保すること

我々はまた、政府省庁間において政策の一貫性が保たれ、調整がとられることを強く希望します。提案されている事前審査制度のセキュリティリスクを評価・判断するための要件を設定する際には、政策立案者は、特定の行動が招く意図しない結果を識別することも含め、個別の決定が全体的な戦略目標と整合しているかを検討する必要があります。また、特定設備や役務を特定社会基盤事業者に提供する事業者を含め、全ての利害関係者に明確となるように、事前の届出において採用される要件や様式が省庁間で統一されていることも重要です。

政策が明瞭かつ明確に定義された基準を採用すること

現代のテクノロジーは、しばしば多国籍な性質を持ち、それに対する脅威もまた同様です。海外で開発されたテクノロジーであるという理由だけで、その技術の取得や導入に対して断定的な禁止をすることは、効果的な政策を実施する上で避けなければなりません。リスク評価基準を明確かつ十分に定義し、国際的なベンチマーク、ベストプラクティス、認証フレームワークを取り入れることを推奨します。クラウドサービスの場合、ISO/IEC 27001、27017、27018、その他の関連規格や第三者認証の取得などが考えられます。国際的に認知された規格や他のプログラムをリスク評価に統合することは、事前審査の効率的かつ効果的な実施を促進し、この新制度の対象となりうる多様な事業者に、より明確で確実な情報を提供することになります。また、国際的に認知された規格に基づく明確かつ十分に定義された基準により、日本政府は最も革新的な製品と競争力のある価格を利用できるようになります。

リスクベースの政策を確保すること

常に進化する脅威環境に、政府機関と企業双方のセキュリティ担当者が適応できるよう、柔軟性のあるリスク管理アプローチを採用することを推奨します。また、的外れな政策による意図しない結果を招くことを避けるためには、リスク管理のアプローチにおいては、悪意ある行為者によるリスクだけでなく、提案された緩和策に関連するリスク、スケジュール、費用を考慮することが重要です。最も重要なことは、悪意ある行為者がその戦術、技術、手順を常に改良していることを認識することです。

結論

BSA は、経済安全保障を効果的に推進するという目標を支援するために、日本政府に協力してゆきたいと考えています。本提言の提出に加え、検討された方向性をよりよく理解し、さらなる提言や提案を通じて政府の目標達成に貢献するためにも、意見交換ができる機会をいただけることを期待しています。